UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/623,488	10/30/2000	Feng Bao	P19949	7274

7055 7590 09/12/2005

GREENBLUM & BERNSTEIN, P.L.C.
1950 ROLAND CLARKE PLACE
RESTON, VA 20191

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/623,488
Filing Date: October 30, 2000
Appellant(s): BAO ET AL.

Attorney: Bruce H. Bernstein
Registration Number: 29,027

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 6/07/2005.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief filed on 06/07/05 is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

The rejection of claims 8 – 18 stands or falls together because appellant's brief does not include a statement that this grouping of claims does not stand or fall together and reasons in support thereof. See 37 CFR 1.192(c)(7).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

5,666,420	Micali	9-1997
5,218,637	Angebaud et al.	6-1993

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 8 – 18 are rejected under 35 U.S.C. 103(a). This rejection is set forth in a prior Office Action, mailed on 08/04/2004.

(11) Response to Argument

Appellant on pages 11 – 15 of the brief argues that MICALI does not disclose "an authentication certificate", "the second party verifying that the encrypted first digital data is an encryption of the first digital data" and "the first party ... sending the encrypted first digital data and the authentication certificate to the second party". Appellant further argues that the combination of MICALI and ANGEBAUD do not disclose, suggest or render obvious the feature recited in claim 8.

In response: Attention is directed to claim 8, which recites "the first party encrypting the first digital data and generating an authentication certificate, the authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data, and sending the encrypted data and the

authentication certificate to the second party; and the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certification ". Even though MICALI teaches simultaneous electronic transactions between two parties that rely on third parties in a minimal and convenient manner, MICALI specifically discloses exchanging digitally signed messages and encrypted or unencrypted digital data only after mutually authentication. ANGEBAUD et al. discloses a method of transferring a secret between two microcomputers and mutually authenticating by exchanging certificates and signatures.

As Appellant recites the limitation with no definition or support for an authentication certificate anywhere in the specification, Examiner takes the broadest interpretation of the claim and interprets "authentication certification" as "An attachment to an electronic message used for security purposes" (Also refer to Exhibit "A", Exhibit "B" Page 2 and Exhibit "C" Abstract). It is well known in the art that the most common use of a (digital) certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. Appellant discloses to exchange a file by way of exchanging of digital signature on a common file (specification pages 7 – 23) and defines a certificate of Encrypted message being a signature. Appellant does not disclose anywhere in the specification how to implement or define an authentication certification and is broadly claiming that the "authentication certificate" recited in claim 8 as an authentication certificate to authenticate that an encrypted digital signature is a digital signature of a particular party and Examiner points to MICALI Column 3 line 61 – Column 4 line 27, Column 5 lines 46 – 48 and

Column 9 lines 4 – 14 for prior art disclosure on authentication certificate and "the first party encrypting the first digital data and generating an authentication certificate, the authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data, and sending the encrypted data and the authentication certificate to the second party", wherein MICALI discloses that at least one communication of the first party to the second party to include generating a (digital) data string and encrypting (digital) data string with an encryption key.

Furthermore, Appellant argues that MICALI does not disclose "the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certification". Examiner points to MICALI Column 5 line 50 – Column 6 line 21 and Column 6 lines 34 – 61, wherein the second party verifying first party's signature and that the encrypted first digital data (encrypted in a way understandable only by second party) is an encrypted first digital data using the authentication certification (second party receives encrypted message, certified version of digital data). As the claim language is broad enough on authentication certification and encrypting first digital data, the combination of MICALI and ANGEBAUD et al. meets the claim as currently recited.

Regarding Claim 9, Appellant argues that MICALI does not disclose "a concatenation of file M_A and a one-way hash of file M_B". Examiner points to MICALI Column 8 lines 51 – 68 and Column 11 lines 52 – 67, the message M (file M_A), is encrypted by actually encrypting M and H(M), where H(M) is a one-way function.

Regarding Claim 10 and 15, Appellant argues that MICALI does not disclose "that the data itself a digital signature (i.e., which is then encrypted and sent to Bob). Examiner points to MICALI Column 4 lines 4 – 14 where at least one communication of the first party to the second party of a data string generated by a process including encrypting a second data string with an encryption key. Examiner further points to MICALI Column 6 lines 1 – 13 for both parties to mutually authenticating the (digital) signature that has been exchanged with the first message (data string).

Regarding Claim 11, Appellant argues that MICALI does not disclose that the recipient should be provided in the form of a "secret file". Examiner points to MICALI Column 1 line 42 – Column 2 line 14 and Column 9 lines 35 – 59, MICALI discloses "a simultaneous ECM (extended certified mail) system with a multiplicity of trustees may make novel use of prior techniques such as fair cryptography, or secret sharing, verifiable secret sharing or threshold cryptosystem". It is well known in the art to encrypt means to encode (scramble) information in such a way that is unreadable to all but those individuals possessing the key to the code and such an encrypted file is a secret file that is exchanged after mutual authentication is disclosed in MICALI. Examiner points to ANGEBAUD Column 1 lines 12 – 14 and Column 9 lines 34 – 61 to explicitly state that a secret file is exchanged between two parties, after mutually exchanging certificate of credentials as well as (digital) signatures.

Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the board to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Pramila Parthasarathy
September 02, 2005

Conferees
Ayaz Sheikh
Supervisory Patent Examiner
Art Unit 2131 & 2136

Chris Revak
Primary Examiner
Art Unit 2131

9/6/05

GREENBLUM & BERNSTEIN, P.L.C.
1950 ROLAND CLARKE PLACE
RESTON, VA 20191